



AF \$ 2/20

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Sancho Enrique David

SYSTEM AND METHOD FOR SECURE NETWORK PURCHASING

Docket No.: 2062.001US1
Filed: February 8, 2000
Examiner: John M. Winter

Serial No.: 09/500,601
Due Date: April 3, 2006
Group Art Unit: 3621

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

We are transmitting herewith the following attached items (as indicated with an "X"):

- Return postcard.
- Appellant's Brief on Appeal (22 pgs.), including authorization to charge the Deposit Account No. 19-0743 in the amount of \$500.00 to pay the Appel Brief fee.

If not provided for in a separate paper filed herewith, Please consider this a **PETITION FOR EXTENSION OF TIME** for sufficient number of months to enter these papers and please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
Customer Number 21186

By: Andrew DeLizio
Atty: Andrew DeLizio
Reg. No. 52,806

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: MS Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 3rd day of April, 2006.

Dawn R. Shaw

Name

Dawn R. Shaw

Signature

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
(GENERAL)



S/N 09/500,601

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant:	Sancho Enrique David	Examiner:	John M. Winter
Serial No.:	09/500,601	Group Art Unit:	3621
Filed:	February 8, 2000	Docket No.:	2062.001US1
		Assignee:	iPass Inc.
Title:	SYSTEM AND METHOD FOR SECURE NETWORK PURCHASING		

APPELLANT'S BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Washington, D.C. 2023 1

This brief is presented in support of the Notice of Appeal filed on October 11, 2005, from the final rejection of pending claims 16-39 of the above-identified patent application. The Final Office Action from which Appellant appeals was mailed July 12, 2005.

Please charge the requisite brief filing fee of \$500.00 to Deposit Account No. 19-0743. Please charge any required additional fees or credit overpayment to Deposit Account No. 19-0743.

Appellant respectfully requests reversal of the Examiner's rejection of pending claims 16-39.

04/07/2006 YPOLITE1 00000065 190743 00500601
01 FC:1402 500.00 DA

APPELLANT'S BRIEF ON APPEAL

Serial Number: 09/500,601

Filing Date: February 8, 2000

Title: SYSTEM AND METHOD FOR SECURE NETWORK PURCHASING

Assignee: iPass Inc.

Page ii
Dkt: 2062.001US1

APPELLANT'S BRIEF ON APPEAL

TABLE OF CONTENTS

1. REAL PARTY IN INTEREST 1

2. RELATED APPEALS AND INTERFERENCES 1

3. STATUS OF THE CLAIMS 1

4. STATUS OF THE AMENDMENTS 1

5. SUMMARY OF THE INVENTIVE SUBJECT MATTER 1

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL 3

7. ARGUMENT 4

 1) THE APPLICABLE LAW 4

 2) DISCUSSION OF THE REJECTION OF CLAIMS 4

8. CONCLUSION 13

CLAIMS APPENDIX: THE CLAIMS ON APPEAL 14

EVIDENCE APPENDIX 19

RELATED PROCEEDINGS APPENDIX 20

PATENT

APPELLANT'S BRIEF ON APPEAL

Serial Number: 09/500,601

Filing Date: February 8, 2000

Title: SYSTEM AND METHOD FOR SECURE NETWORK PURCHASING

Assignee: iPass Inc.

Page 1
Dkt: 2062.001US1

1. REAL PARTY IN INTEREST

The real party in interest of the above-captioned patent application is the assignee, iPass Inc.

2. RELATED APPEALS AND INTERFERENCES

Appellant knows of no other appeals or interferences which will have a bearing on the Board's decision in the present appeal.

3. STATUS OF THE CLAIMS

Claims 16-39 have been rejected twice and are the subject of the present appeal.

4. STATUS OF THE AMENDMENTS

No amendments were filed after the final rejection mailed July 12, 2005.

5. SUMMARY OF THE INVENTIVE SUBJECT MATTER

This summary is presented in compliance with the requirements of Title 37 C.F.R. § 41.37(c)(1)(v), mandating a “concise explanation of the subject matter defined in each of the independent claims involved in the appeal ...” Nothing contained in this summary is intended to change the specific language of the claims described, nor is the language of this summary to be construed so as to limit the scope of the claims in any way.

Claim 16

Claim 16 is supported in Figure 7 and in the specification *inter alia* at page 16, paragraph “a” through page 17, paragraph “e”.

Figure 7 is a block diagram illustrating a technique for verifying a user and a user computer. The technique can include receiving, in a verification computer, a request for verification from a computer and, in response to the request for verification, sending at least one request to the user computer. The technique can also include receiving at least one response from the user computer, the at least one response including a first fingerprint file. The specification describes that the response can also include a first identification for the user, said first fingerprint file-including at least one identifying characteristic of the user computer. The specification also describes that the technique, to verify the user computer, can include comparing the first fingerprint file against a second fingerprint file, the second fingerprint file accessible by the verification computer, said second fingerprint file including at least one identifying characteristic of a user computer. The specification also describes that the technique can include comparing the first identification for the user against a second identification for the user to verify the user, the second identification for the user accessible by the verification computer and sending at least one verification response, based upon the comparing of the first fingerprint file against the second fingerprint file and upon the comparing of the first identification for the user against the second identification for the user.

Claim 34

Claim 34 is supported in Figure 7 and in the specification *inter alia* at page 16, paragraph “a” through page 17, paragraph “e”.

Figure 7 is a block diagram illustrating a computer for verifying a user and a user computer. The diagram illustrates that the computer can receive information from a user computer, the information including a second fingerprint file. The diagram also illustrates that the computer can receive information indicative of first fingerprint file. The specification indicates that the computer can also receive a first identification for the user and that said first fingerprint file can include at least one identifying characteristic of the user computer. The specification describes that the computer can compare information indicative of the second fingerprint file and the second identification for the user with information indicative of the first fingerprint file and first identification for the user, and to cause a message to be generated based upon the comparing.

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The grounds for review are whether claims 16-39 were properly rejected under 35 U.S.C. § 103(a) as being unpatentable over Padgett et al. (U.S. 6,167,518) in view of Ross (U.S. 6,195,447) and further in view of Beetcher et al. (U.S. 5,933,497).

7. ARGUMENT

Claims 16-39 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Padgett et al. (U.S. 6,167,518) in view of Ross (U.S. 6,195,447) and further in view of Beetcher et al. (U.S. 5,933,497). Appellant respectfully traverses this rejection because the Examiner has not made a *prima facie* case of obviousness.

1) *The Applicable Law*

According to *M.P.E.P.* § 2141, which cites *Hodosh v. Block Drug Co., Inc.*, 786 F.2d 1136, 1143 n.5, 229 USPQ 182, 187 n.5 (Fed. Cir. 1986), the following tenets of patent law must be adhered to when applying 35 U.S.C. § 103. First, the claimed invention must be considered as a whole. Second, the references must be considered as a whole and must suggest the desirability and thus the obviousness of making the combination. Third, the references must be viewed without the benefit of impermissible hindsight vision afforded by the claimed invention. Fourth, obviousness is determined using a reasonable expectation of success standard. Under § 103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. *M.P.E.P.* § 2141 (citing *Graham v. John Deere*, 383 U.S. 1, 148 USPQ 459 (1966)).

The Examiner has the burden under 35 U.S.C. § 103 to establish a *prima facie* case of obviousness. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *M.P.E.P.* § 2142 (citing *In re Vaeck*, 947 F.2d, 488, 20 USPQ2d 1438 (Fed. Cir. 1991)).

The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. *M.P.E.P.* § 2142 (citing *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)). The references must expressly or impliedly suggest the claimed invention or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references. *M.P.E.P.* § 2142 (citing *Ex parte Clapp*, 227 USPQ 972, 973 (Bd. Pat. App. & Inter. 1985)). In considering the disclosure of a reference, it is proper to take into account not only specific teachings of the reference but also the inferences which one skilled in the art would reasonably be expected to draw therefrom. *M.P.E.P.* § 2144.01 (citing *In re Preda*, 401 F.2d 825, 826, 159 USPQ 342, 344 (CCPA 1968)). However, if the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *M.P.E.P.* § 2143.01 (citing *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984)).

In order to take into account the inferences which one skilled in the art would reasonably make, the examiner must ascertain what would have been obvious to one of ordinary skill in the art at the time the invention was made, and not to the inventor, a judge, a layman, those skilled in remote arts, or to geniuses in the art at hand. *M.P.E.P.* § 2141.03 (citing *Environmental Designs*,

Ltd. v. Union Oil Co, 713 F.2d 693, 218 USPQ 865 (Fed. Cir. 1983), *cert. denied*, 464 U.S. 1043 (1984)).

The examiner must step backward in time and into the shoes worn by the hypothetical “person of ordinary skill in the art” when the invention was unknown and just before it was made. In view of all factual information, the examiner must then make a determination whether the claimed invention “as a whole” would have been obvious at that time to that person. Knowledge of applicant’s disclosure must be put aside in reaching this determination, yet kept in mind in order to determine the “differences,” conduct the search and evaluate the “subject matter as a whole” of the invention. The tendency to resort to “hindsight” based upon applicant’s disclosure is often difficult to avoid due to the very nature of the examination process. However, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art. *M.P.E.P.* § 2141.03.

2) Discussion of the rejection of claims

THE REFERENCES DO NOT TEACH OR SUGGEST ALL THE CLAIM ELEMENTS

Discussion of Claims 16-33

Claim 16 recites, “receiving at least one response from the user computer, the at least one response including a first fingerprint file and a first identification for the user.... said first fingerprint file including at least one identifying characteristic of the user computer” The Examiner admits, “Padgett et al (‘518) does not explicitly disclose the features of ... receiving at least one response from the user computer, the at least one response including a first fingerprint file and a first identification for the user.” Office Action mailed 12/17/2004 at page 2 (hereafter referred to as Office Action). However, the Examiner asserts that Ross discloses these claim features at column 3, lines 1-6 and column 2, lines 61-67. *Id.*

Appellant respectfully submits that the Examiner has mischaracterized Ross. In particular, the cited passages do not mention “a first fingerprint file *and a first identification for*

the user... said first fingerprint file including at least one identifying characteristic of the user computer.” (Emphasis added.) In contrast, Ross’ passage at column 3, lines 56-59 states,

“At the local site 40, a processor 42 receives the scanned fingerprint image data from the scanner 32 across the transmission line 26 and acts to locate the real-time discrete topographical minutia points.”

Furthermore, Ross’ passage at column 2, lines 19-33 states,

A database memory interacts with the processor for storing a historical image file corresponding to the applied fingerprint. The historical image file comprises respective statistical representations of respective spatial relationships between the minutia points. The statistical representations are acquired through repeated detection and statistical analysis of the applied fingerprint. The local site further includes a comparator for identifying the real time physical relationship against the corresponding statistical spatial relationship and verifying the applied fingerprint as authentic where the real time physical relationship is not less than a predetermined minimum deviation from the statistical spatial relationship corresponding to the fingerprint plasticity and not greater than a predetermined maximum deviation from the statistical spatial relationship corresponding to a different fingerprint.

Neither of the cited passages teaches or suggests “a first fingerprint file and a first identification for the user” where the first fingerprint file includes “*at least one identifying characteristic of the user computer.*” See claim 16. Moreover, Appellant cannot find any other passage in Ross that teaches these claim features.

Claim 16 also recites, “comparing the first fingerprint file against a second fingerprint file, *to verify the user computer.*” (Emphasis added.) The Examiner asserts that Ross discloses this claim feature at column 4, lines 1-7. However, Appellant respectfully submits that the Examiner has again mischaracterized Ross. Ross’ passage at column 4, lines 1-14 states,

The processor 42 also connects to a fingerprint database memory 44 to assist in maintaining accurate criteria for subsequent comparison of the real time feature vector to previously detected feature vectors. The processor statistically analyzes the real time feature vector as an individual sample with respect to a history file for the particular fingerprint. The history file is

accessed from the fingerprint database memory and includes statistical criteria comprising mean values of physical relationships between predetermined minutia, or calculated standard deviations between minutia. The file is statistically updated each time the corresponding fingerprint is successfully utilized to gain access to the secured area and is transmitted back to the database memory for storage. (Emphasis added.)

This passage teaches processing a fingerprint to gain access to a secured area. However, the passage does not teach “comparing the first fingerprint file against a second fingerprint file, *to verify the user computer.*” See claim 16. Appellant cannot find any other passages in Ross that teach this claim feature. The Examiner further asserted, “the feature of comparing fingerprint files in order to verify the identity of the user is more clearly shown in column 2, lines 19-34, [where] Ross is comparing a captured fingerprint against a historical database, thusly verifying the identity of the user.” (Insertion added.) Office Action at page 2. However, Appellant again points out that the passage does not teach or suggest verifying the “**user computer,**” as recited in claim 16.

Claim 16 also recites, “sending at least one verification response, based upon the comparing of the first fingerprint file against the second fingerprint file and upon the comparing of the first identification for the user against the second identification for the user.” In claim 16, the verification response is based on two comparisons: 1) comparison of the first and second fingerprint files; and 2) comparison of the first and second user identifications. The Examiner asserts Ross teaches these claim features at column 4, lines 25-27. See Office Action at page 4. Ross’ passage at column 4, lines 25-27 states, “the comparator generates a verification signal for transmission across the transmission line 28 to the access mechanism 34 to admit or deny entry to the secured area.” Although this passage teaches a verification signal, it does not teach or suggest sending a verification response based on comparison of the first and second fingerprint files *and comparison of the first and second user identifications*, as recited in claim 16. Appellant cannot find any other passage in Ross that teaches this claim feature.

For the combination of Padgett, Ross, and Beetcher to teach or suggest all the elements of claim 16, Padgett and Beetcher must teach what Ross is lacking. The Examiner does not point to a passage in Padgett or Beetcher that teaches or suggests the claim features discussed above. As a result, for at least the reasons noted above, Appellant respectfully submits the combination of Padgett, Ross, and Beetcher does not teach or suggest all the elements of independent claim 16.

Claims 17-33 each depend directly or indirectly on independent claims 16. As such, they each include the claim elements discussed above. For at least the reasons noted above, Appellant respectfully submits that the combination of Padgett, Ross, and Beetcher does not teach or suggest all the elements of dependent claims 17-33.

Discussion of Claim 34-39

Claim 34 recites, “a processor for communicating with the storage unit and the memory unit to compare information indicative of the second fingerprint file and the second identification for the user with information indicative of the first fingerprint file and first identification for the user.” (Emphasis added.) The Examiner asserts Padgett teaches these claim features in the passages at column 2, lines 61-67 and column 3 lines 1-6. See Office Action at page 7.

Padgett's passage at column 2, line 61 to column 3, line 6 states,

The digital representation of the registrant's biological indicia is encrypted using the registrant's private key and sent to the certificate authority along with the registrant's public key. The certificate authority decrypts the digital representation and stores it. The registrant then visits a remote registration terminal in person with the digital representation and other identifying documents. The operator of the remote registration terminal verifies the identity of the registrant from the identifying documents and transmits the digitized representation to the certificate authority. The certificate authority compares the decrypted digital representation with the representation sent from the remote registration terminal.

This passage describes comparing two items. Padgett's certificate authority compares decrypted biological information with information sent from a remote terminal. However, claim 34's processor compares four items. In particular, claim 34's processor is to compare information indicative of the second fingerprint file and the second identification for the user with information indicative of the first fingerprint file and first identification for the user. Therefore, this passage does not teach or suggest the processor of claim 34. Appellant cannot find any other passages in Padgett that teach this claim feature.

Additionally, claim 34 recites, "a storage unit to store information received from a user computer, the information including *a second fingerprint file and a second identification for a user*." (Emphasis added.) Claim 34 also recites, "a memory unit to receive information indicative of *a first fingerprint file and a first identification for the user*." The Examiner asserts Ross discloses these claim features at column 3, lines 56-59. See Office Action at page 7. Ross' passage at column 3, lines 56-59 states, "At the local site 40, a processor 42 receives the scanned fingerprint image data from the scanner 32 across the transmission line 26 and acts to locate the real-time discrete topographical minutia points." This passage clearly does not teach or suggest the claimed storage and memory units. Moreover, Appellant cannot find any other passages in Ross that teaches these claim features.

Claim 34 recites first and second fingerprint files, where each fingerprint file includes at least one identifying characteristic of a user computer. The Examiner admits that Beetcher does not include a second fingerprint file. See Office Action at page 7. However, the Examiner asserts that a second fingerprint file would have been obvious "since it has been held that mere duplication of the essential working parts of a device involves only routine skill in the art." Office Action at page 7, citing *St. Regis Paper Co. v. Bemis Co.*, 193 USPQ8. The Examiner's position assumes the claimed invention has merely added a second fingerprint file to a well-known device. On the contrary, the claimed invention includes 1) first and second fingerprint files that include at least one identifying characteristic of a user computer and 2) a processor for

APPELLANT'S BRIEF ON APPEAL

Serial Number: 09/500,601

Filing Date: February 8, 2000

Title: SYSTEM AND METHOD FOR SECURE NETWORK PURCHASING

Assignee: iPass Inc.

Page 11
Dkt: 2062.001US1

performing operations based on the second fingerprint file. As such, the claimed invention has not merely duplicated the essential working parts of a device, but has created a patentable clearinghouse computer.

Claims 35-39 each depend directly or indirectly on independent claims 34. As such, they each include the claim elements discussed above vis-à-vis claim 34. For at least the reasons noted above, Appellant respectfully submits that the combination of Padgett, Ross, and Beetcher does not teach or suggest all the elements of dependent claims 35-39.

THERE IS NO SUGGESTION TO COMBINE BEETCHER WITH PADGETT AND ROSS

Beetcher describes techniques for restricting the ability of a computer user to use licensed software in a manner inconsistent with the license (see Beetcher at column 1, lines 7-11), whereas Padgett teaches using biometric information to authenticate electronic messages (see Padgett at column 1, lines 6-11). Ross teaches a system for authenticating human fingerprints. See Ross at Abstract. The Examiner has improperly combined Beetcher with Padgett and Ross. For a proper combination, the Examiner must show that some objective teaching in the prior art or some knowledge generally available to one of ordinary skill in the art would lead an individual to combine the relevant teaching of the references. *In re Fine*, F.2d 1071, 1074, 5 USPW2d 1596, 1598 (Fed. Cir. 1988).

The *Fine* court stated,

Obviousness is tested by "what the combined teaching of the references would have suggested to those of ordinary skill in the art." *In re Keller*, 642 F.2d 413, 425, 208 USPQ 871, 878 (CCPA 1981)). But it "cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination." *ACS Hosp. Sys.*, 732 F.2d at 1577, 221 USPQ at 933. And "teachings of references can be combined *only* if there is some suggestion or incentive to do so." *Id.* (emphasis in original).

APPELLANT'S BRIEF ON APPEAL

Serial Number: 09/500,601

Filing Date: February 8, 2000

Title: SYSTEM AND METHOD FOR SECURE NETWORK PURCHASING

Assignee: iPass Inc.

Page 12
Dkt: 2062.001US1

The Examiner asserts that one of ordinary skill in the art would combine Beetcher with Padgett and Ross “in order to increase security and systems that utilize unique hardware identifiers.” Office Action at page 7. However, this assertion is unfounded, as the Examiner did not identify a single passage in any of the references that teaches or suggests combining Beetcher with Padgett and Ross. Furthermore, the Examiner did not explain how the references could be combined based a combination of knowledge of one of ordinary skill in the art and the nature of the problem to be solved. Because there is no teaching or suggestion to combine the cited references, Appellant submits that the combination is improper. As such, reversal of the Examiner’s rejection of claims 16-39 is hereby requested.

APPELLANT'S BRIEF ON APPEAL

Serial Number: 09/500,601

Filing Date: February 8, 2000

Title: SYSTEM AND METHOD FOR SECURE NETWORK PURCHASING

Assignee: iPass Inc.

Page 13
Dkt: 2062.001US1

8. CONCLUSION

It is respectfully submitted that the claimed invention is not unpatentable in view of the cited art. It is respectfully submitted that claims 16-39 should therefore be allowed. Reversal of the Examiner's rejections of claims 16-39 is respectfully requested.

Respectfully submitted,

Andrew Warner

By his Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER &
KLUTH, P.A.

P.O. Box 2938

Minneapolis, MN 55402

(612) 373-6909

Date 4/3/2006 By Andrew DeLizio

Andrew DeLizio
Reg. No. 52,806

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop AF, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 3 day of April, 2006.

Dawn R. Shaw

Dawn R. Shaw

Name

Signature

CLAIMS APPENDIX: THE CLAIMS ON APPEAL

16. (Rejected) A method for verifying a user and a user computer comprising:
receiving, in a verification computer, a request for verification from a computer;
in response to the request for verification, sending at least one request to the user computer;
receiving at least one response from the user computer, the at least one response
including a first fingerprint file and a first identification for the user, said first fingerprint file
including at least one identifying characteristic of the user computer;
comparing the first fingerprint file against a second fingerprint file, to verify the user
computer, the second fingerprint file accessible by the verification computer, said second
fingerprint file including at least one identifying characteristic of a user computer;
comparing the first identification for the user against a second identification for the user
to verify the user, the second identification for the user accessible by the verification computer;
and
sending at least one verification response, based upon the comparing of the first
fingerprint file against the second fingerprint file and upon the comparing of the first
identification for the user against the second identification for the user.
17. (Rejected) The method according to claim 16 wherein the verification computer is a
clearinghouse computer.
18. (Rejected) The method according to claim 16 wherein the verification computer is a
vendor computer.

19. (Rejected) A method according to claim 16, wherein said sending of at least one request to a user computer includes:

- sending a first request to the user computer for the first fingerprint file; and
- sending a second response to the user computer for the first identification for the user.

20. (Rejected) A method according to claim 16, wherein said receiving of at least one response from the user computer includes:

- receiving a first response from the user computer including the fingerprint file; and
- receiving a second response from the user computer including the first identification for the user.

21. (Rejected) A method according to claim 20, wherein the second response from the user computer is received prior to first response from the user computer.

22. (Rejected) A method according to claim 16, wherein said comparing of the first fingerprint file against a second fingerprint file, and comparing the first identification for the user against a second identification for the user are not performed simultaneously.

23. (Rejected) A method according to claim 18, wherein said sending of at least one response to the vendor computer, based upon the comparing of the first fingerprint file against the second fingerprint file and upon the comparing of the first identification for the user against the second identification for the user includes sending a confirmation only when both the first fingerprint file and the first identification of the user match the second fingerprint file and the second identification for the user respectively.

24. (Rejected) A method according to claim 19, wherein said receiving of at least one

response from the user computer includes:

receiving a first response from the user computer including the first fingerprint file; and
receiving a second response from the user computer including the first identification for

the user.

25. (Rejected) A method according to 24, wherein the second response from the user computer is received prior to the first response from the user computer.

26. (Rejected) A method according to claim 16, wherein the first identification for the user includes a password.

27. (Rejected) A method according to claim 16, wherein the first fingerprint file includes information based upon an identification number of a CPU of the user computer.

28. (Rejected) A method according to claim 16, wherein the first fingerprint file includes information based upon a MAC address associated with the user computer.

29. (Rejected) A method according to claim 16, wherein prior to the receiving of the first request from the verification computer,

storing the second fingerprint file in a first data base accessible by verification computer, and

storing the second identifications for the user in a second database accessible by the verification computer.

30. (Rejected) A method according to claim 18, wherein prior to the receiving of the first request from the vendor computer,

storing the second fingerprint file in a first data base accessible by a clearinghouse computer, and

storing the second identifications for the user in a second database accessible by a clearinghouse computer.

31. (Rejected) A method according to claim 28, wherein the first database and second database are the same.

32. (Rejected) A method according to claim 18, wherein the receiving of a request from a vendor computer includes receiving an internet address of the user computer.

33. (Rejected) A method according to claim 32, wherein prior to the sending of the at least one request to the user computer, identifying the user computer based upon the internet address received from the vendor computer.

34. (Rejected) A clearinghouse computer comprising:

a storage unit to store information received from a user computer, the information including a second fingerprint file and a second identification for a user, said second fingerprint file including at least one identifying characteristic of a user computer;

a memory unit to receive information indicative of first fingerprint file and a first identification for the user said first fingerprint file including at least one identifying characteristic of the user computer; and

a processor to communicate with the storage unit and the memory unit, to compare information indicative of the second fingerprint file and the second identification for the user with information indicative of the first fingerprint file and first identification for the user, and to cause a message to be generated based upon the comparing.

35. (Rejected) A clearinghouse computer according to claim 34, wherein the storage unit includes:

- a first storage location to store the second fingerprint file, and
- a second storage location to store the second identification for the user.

36. (Rejected) A clearinghouse computer according to claim 34, wherein the memory unit includes:

- a first memory location to store, at least temporarily, the first fingerprint file, and
- a second memory location to store, at least temporarily, the first identification for the user.

37. (Rejected) A clearinghouse computer according to claim 34, further including:
an output to receive the message to be generated based upon the comparison, and
the output further to communicate with a vendor computer.

38. (Rejected) A clearinghouse computer according to claim 34, wherein the second identification for the user includes a password.

39. (Rejected) A clearinghouse computer according to claim 34, wherein the second fingerprint file includes information based upon an identification number of a CPU of the user computer.

APPELLANT'S BRIEF ON APPEAL

Serial Number: 09/500,601

Filing Date: February 8, 2000

Title: SYSTEM AND METHOD FOR SECURE NETWORK PURCHASING

Assignee: iPass Inc.

Page 19

Dkt: 2062.001US1

EVIDENCE APPENDIX

NONE

APPELLANT'S BRIEF ON APPEAL

Serial Number: 09/500,601

Filing Date: February 8, 2000

Title: SYSTEM AND METHOD FOR SECURE NETWORK PURCHASING

Assignee: iPass Inc.

Page 20

Dkt: 2062.001US1

RELATED PROCEEDINGS APPENDIX

NONE